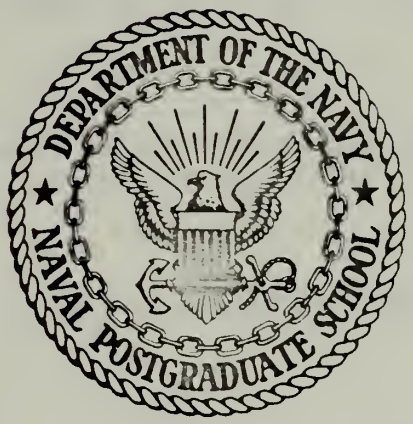
DESIGN OF A REMOTELY CONTROLLED PSEUDO-RANDOM GENERATOR WITH LOCAL TIME GATING

Gordon Franklin Gilbert

NAVAL POSTGRADUATE SCHOOL
Monterey, California



THESIS

DESIGN OF A REMOTELY CONTROLLED PSEUDO-RANDOM GENERATOR WITH LOCAL TIME GATING

by

Gordon Franklin Gilbert, Jr.

Thesis Advisor: G. A. Myers

December 1971

Approved for public release; distribution unlimited.

Design of a Remotely Controlled Pseudo-Random Generator With Local Time Gating

by

Gordon Franklin Gilbert, Jr.
Lieutenant, United States Navy
B.S., University of Missouri, 1965

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
December 1971

ABSTRACT

This study considers the design of a remote-controlled feedback shift register (pseudo-random sequence generator). A coded sequential input is used to modify existing feedback switch connections. The free running shift register then generates a different maximal length pseudo-random sequence. To prevent control or use of the device by unauthorized persons, a time gate is included in the operation. Recommendations for implementation are presented.

TABLE OF CONTENTS

LIST OF DRAWINGS

I. INTRODUCTION

A. BACKGROUND

A shift register that is clocked without an input will eventually assume and maintain an all zero output. However, if outputs of the registers are fed back to the first stage then the output may, if the proper feedback is selected, form a periodic sequence. In particular if the feedback is a modulo two adder and the initial state of all zeros is prohibited then the register becomes a linear feedback shift register (LFSR) [Ref. 1].

The maximum number of states of such a register is 2^N-1, where N is the total number of storage devices (shift register stages). When the feedback is set so that all of these states are reached in the periodic cycle the output of the last stage becomes a maximally long binary sequence with period $\tau(2^N-1)$, where τ is the clock period. In this manner a sequence much longer than that determined by the number of register stages is possible.

Of particular importance are the following properties of the sequence. First, the number of one binary state (0) approximately equals the number of occurences of the other state (1). Specifically the difference is one. Secondly, the length of consecutive occurences (runs) of a state follows a geometric progression, i.e. one-half of the runs have length one, one-fourth have length two, one-eighth have length three, etc. Finally, the expected value of the autocorrelation function is two-valued with a pronounced peak at the origin. Therefore these sequences are random like or pseudo-random.

The construction of FSR's to generate a specified long sequence with these properties is widely understood. A detailed study of these devices may be found in Refs. 1-3.

Such generators find applications in a diversity of fields including radar ranging, secure or private communications, signal acquisition, and random number generation. References 4-8 contain examples of specific applications. In this report we consider an application of the LFSR in secure communications.

B. FUNDAMENTAL PARAMETERS

The four predominating physical and electrical parameters that characterize the LFSR and its sequence are the clock rate, initial conditions, feedback connections and number of stages in the shift register.

The clock period determines the time duration of the sequence and affects the bandwidth of a signal modulated by a pseudo-random sequence.

The initial condition of each register stage determines the starting point in the sequence.

The number N of storage elements of the register sets an upper bound 2^N-1 on the length of the sequence from an unclocked LFSR.

The feedback network controls the sequential state flow and, under certain conditions, the length of the cycle. For purposes of this report the feedback is an output from every stage through an electronic switch to a modulo two adder. The output of the adder is returned to the first state.

To change from one sequence to another, either the feedback configuration switches may be changed or the number of stages may be modified. With the assumption that a change in the sequence length is not desired and that it remain maximum, feedback switching transitions that yield a

new modulo two primitive polynomial are required [Ref. 1]. Therefore, all of the 2^N variations in feedback are not allowed. For example, a twenty stage LFSR has over a million switch permutations. Of these, 24,000 yield a maximal-length sequence. Therefore even with the maximal length requirement, a considerable library of sequences is available with nominal register length.

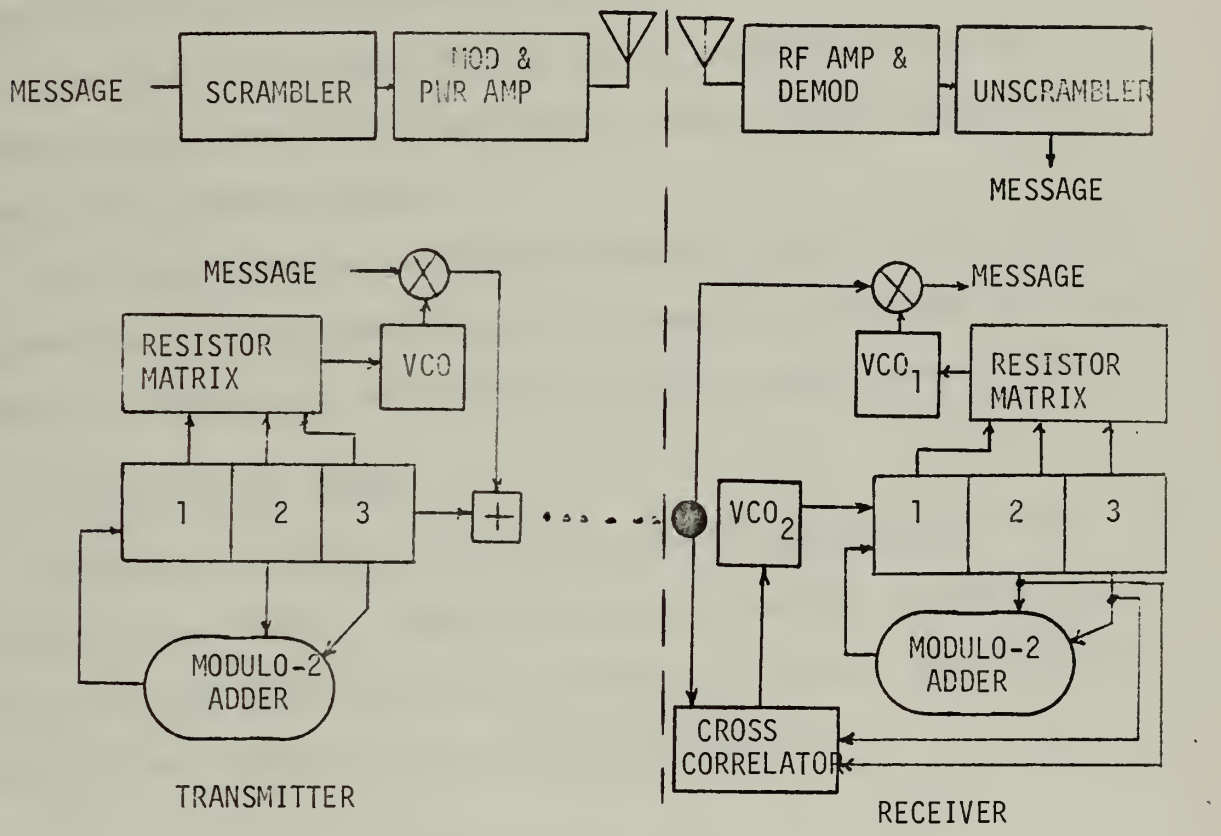


Figure 1. Transmitter-Receiver with Scrambler, Simplified

The use of the LFSR and the reason for insertion of the electronic switches in the feedback paths can best be summarized after examining Figure 1. In the transmitter the LFSR is stepping through the sequence 111, 011, 001, 100, 010, 101, and 110 with an output sequence 1110010. The states of the registers control the frequency of the mixing voltage controlled oscillator (VCO) through the resistive matrix. The output of the mixer, a scrambled analog signal, is added to a low level sequence, filtered and transmitted. Assuming the resistive matrices are matched

the signal can be recovered by the synchronized output of VCO_1. Synchronization is effected through the cross correlator — VCO_2 clock [Ref. 8].

If in the transmitter the feedback from stage 2 is transferred to stage 1 the sequence length remains the same but the cycle is changed. The receiver can no longer be synchronized.

Insertion of electronic switches in the feedback paths of the receiver would permit the transmitter to signal its new configuration and affect a feedback match.

This report considers a method of remotely controlling the feedback connections of a LFSR when certain environmental restrictions are imposed. Such an arrangement is useful when considering secure communications.

C. CONTENTS OF THE REPORT

Section II defines a set of constraints placed on receiver FSR configuration changes. A design proposal is presented in Section III that satisfies these constraints. Section IV discusses implementation and Section V summarizes the conclusions reached.

II. PROBLEM SPECIFICATIONS

The problem of interest results from an examination of a situtation involving several transmit-receive units similar to that described in Section I. Under normal conditions the requirement for a remote controlled switching unit would be unnecessary. An operator at each location is either told the next configuration or consults a time table of switch settings. There are situations where auch a priori knowledge is not feasible or not permitted. The most obvious of these is unattended operation e.g. operation in an uninhabitable environment (deep space) or the operator may be present but have so many constraints imposed on his actions as to preclude matching his unit. It is the latter situation under consideration. The constraints imposed by this study are:

(1) No open signal designating the new configuration will be transmitted using the old configuration.

(2) No chart, table, card, or module may be present at the operator's location.

(3) Switch select buttons that give direct access to the LFSR are forbidden.

(4) There must be positive assurance that at operator is present when a change is effected.

(5) There must be a high probability that the operator is authorized to accept a configuration change.

In the following development it is assumed that a master unit capable of manual modification exists and that a method of coding and decoding a change signal is available.

The next section considers a solution to the problem stated and satisfying the constraints imposed.

III. PROPOSED SOLUTION

The solution to the problem in Section II requires a positive action by the operator to indicate his presence and acceptability. Since he is expected to perform this action from memory it should be simple but at the same time exclusive enough to serve as an identity index.

Since at the time immediately prior to his action information necessary for correlation by the receiver is lost it is assumed that a different demodulation technique (separate receiver) is available for change-information transmission.

When the transmission is restricted to a small preset time frame and the necessary knowledge of this time frame is presumed known only to assigned operators he may accept data to effect a change by proper operation of switch S_1 in Fig. 2.

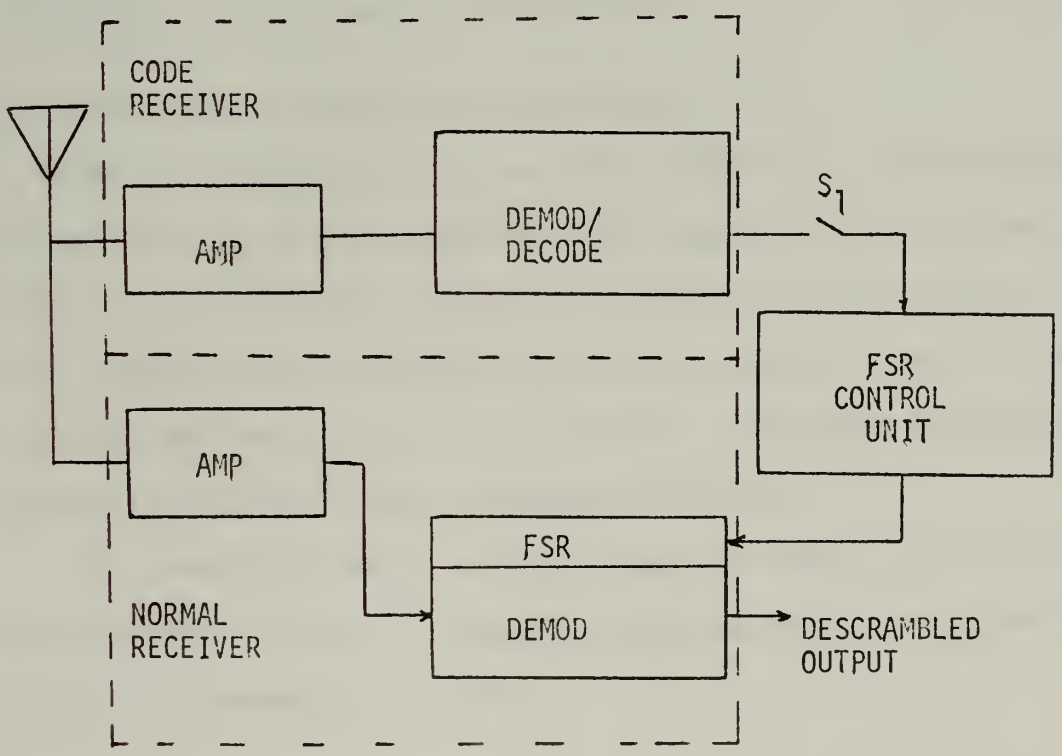


Figure 2. Dual Receiver with Control Unit

It is the responsibility of the control unit of Fig. 2 to decide whether his action is proper. A block diagram for a possible control unit that will accomplish this is shown in Fig. 3.

In Fig. 3. the receiver-buffer link is broken by switch S_1. With the switch closed the control unit is capable of accepting a digital input to a storage device and then performing the required logic to furnish the multiple outputs to the feedback network of the shift register. If the switch remains on for a fixed time a disable pulse is sent to the register. Therefore, successful operation requires switch S_1 be opened and closed in particular, established time windows. In effect the operator actuates a locally controlled time gate in accordance with exclusive a priori knowledge. The change of feedback connections is set by the information contained in the input pulse train he controls.

A particular control unit with necessary coupling, feedback logic, timing and FSR is expanded in the following sections. This example is introduced for illustrative purposes only.

A. FEEDBACK-SHIFT REGISTER AND SWITCHING LOGIC

The FSR considered here is an eight stage unit. This register with transmission gates and modulo two adder (exclusive OR) is shown in Fig. 4. The transmission gates are electronic devices capable of very low impedances when the control state (S) is high (1) and are open circuits when the control state is low (0). Reference 12 describes a COSMOS fabrication of such a transmission gate.

The irreducible modulo two polynomials of degree less than twelve are tabulated in Ref. 1. From this table the following sixteen irreducible polynomials are derived:

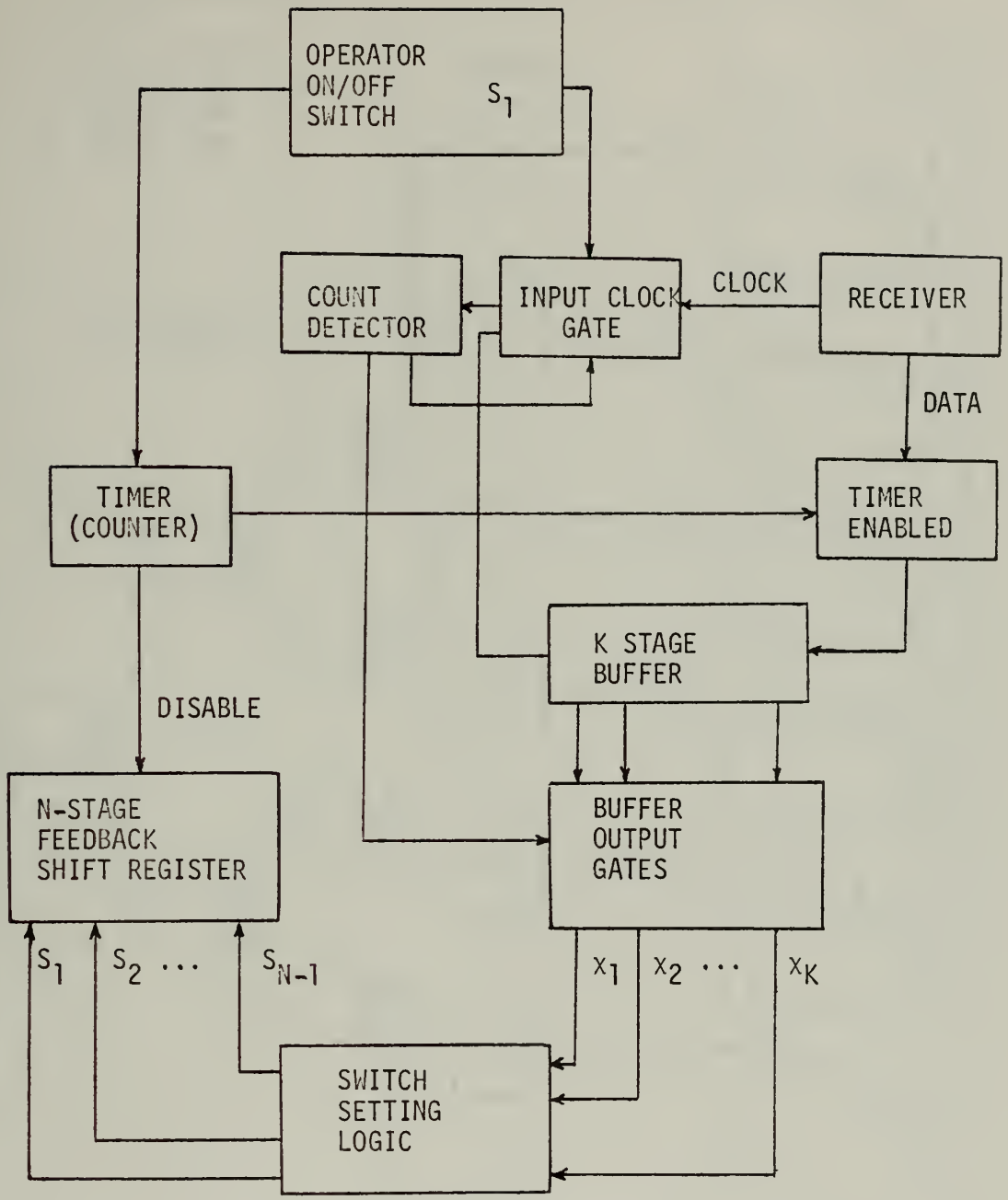


Figure 3. Control Unit Block Diagram

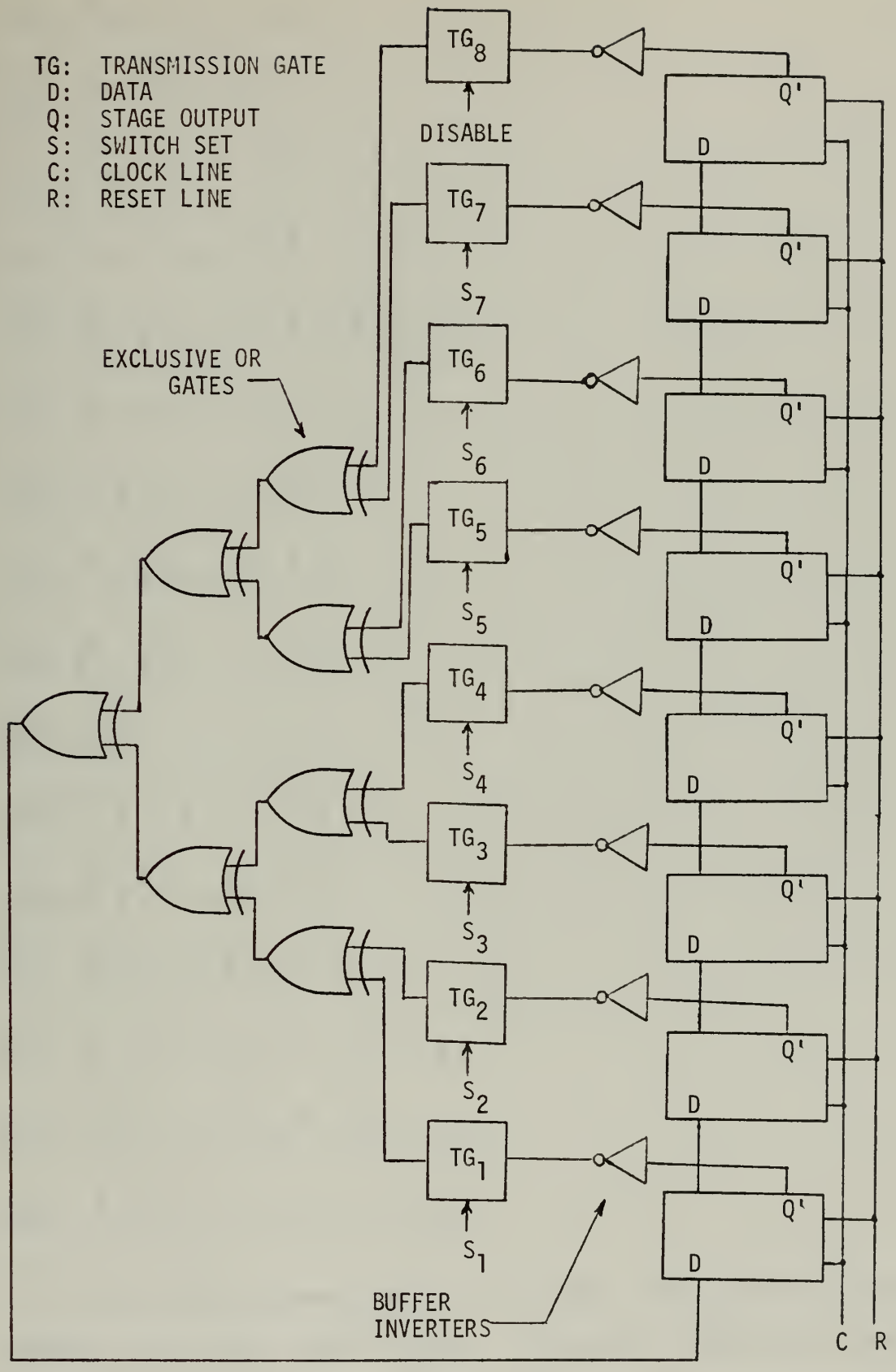


Figure 4. Shift Register, Transmission Gates, and Modulo-two Adder

(1) $x^8 + x^4 + x^3 + x^2 + 1$

(2) $x^8 + x^5 + x^3 + x + 1$

(3) $x^8 + x^5 + x^3 + x^2 + 1$

(4) $x^8 + x^6 + x^3 + x^2 + 1$

(5) $x^8 + x^6 + x^4 + x^3 + x^2 + x + 1$

(6) $x^8 + x^6 + x^5 + x + 1$

(7) $x^8 + x^6 + x^5 + x^2 + 1$

(8) $x^8 + x^6 + x^5 + x^3 + 1$

(9) $x^8 + x^6 + x^5 + x^4 + 1$

(10) $x^8 + x^7 + x^2 + x + 1$

(11) $x^8 + x^7 + x^3 + x^2 + 1$

(12) $x^8 + x^7 + x^5 + x^3 + 1$

(13) $x^8 + x^7 + x^6 + x + 1$

(14) $x^8 + x^7 + x^6 + x^3 + x^2 + x + 1$

(15) $x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$

(16) $x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1$

This listing represents all of the maximal length generating polynomials for an eight stage register. The actual feedback taps requiring closed electronic transmission gates are then derived from the relation:

$$\text{CLOSED } S_{ji} = N - i \qquad i = \{\text{Exponents} \neq N\}$$
$$j = 1, 2, \ldots, 16$$

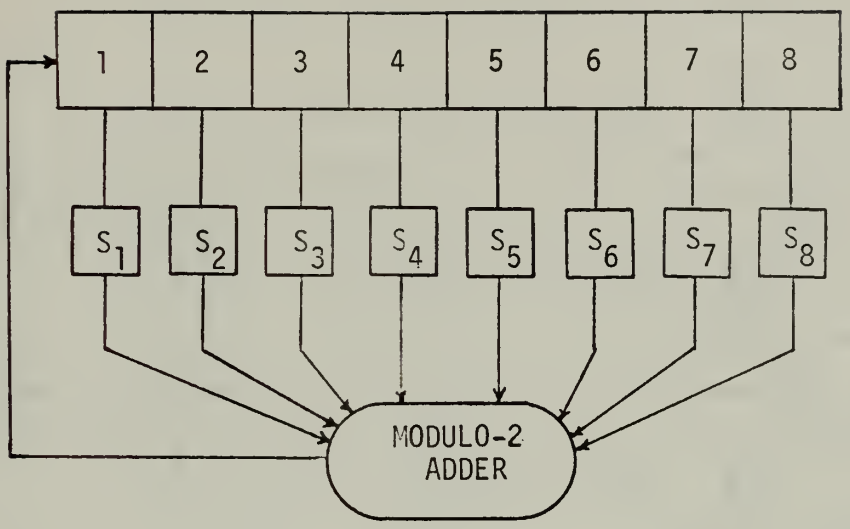
These sixteen switch selection formulas are then binary coded to form a four input, eight output logic table. Figure 5 includes this table with a simplified representation of the FSR. Configuration 0000 is designated Code 0 because of the particular significance it plays in the configuration change cycle.

From this table it can be seen that the eighth stage, or serial output stage, is always closed. This is characteristic of maximal length sequence generation.

Therefore the necessary switching to change a sequence results in a four input, seven output logic function. Figure 6 represents a NAND circuit that will achieve the required switching. It should of course be minimized before being used [Ref. 11]. Attempts to reduce this logic network by hand computation to a minimal cost two level NAND circuit gave inconsistent results. Since its minimization was not necessary for development of the concept it was kept in its present form. However the attempt did demonstrate that even more complicated multiple input-multiple output networks require computer-assisted design.

B. INPUT GATING AND STORAGE

To furnish driving inputs for the switching logic network and to insure that they hold their desired level a static buffer register was chosen as storage for the receiver inputs. To insure that spurious receiver clock pulses do not upset a code that has been set, feedback from a counter gates the receiver clock out when the required number of



CONFIGURATION				SWITCH POSITION							
a	b	c	d	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
0	0	0	0	0	0	0	1	1	1	0	1
0	0	0	1	0	0	1	0	1	0	1	1
0	0	1	0	0	0	1	0	1	1	0	1
0	0	1	1	0	1	0	0	1	1	0	1
0	1	0	0	0	1	0	1	1	1	1	1
0	1	0	1	0	1	1	0	0	0	1	1
0	1	1	0	0	1	1	0	0	1	0	1
0	1	1	1	0	1	1	0	1	0	0	1
1	0	0	0	0	1	1	1	0	0	0	1
1	0	0	1	1	0	0	0	1	0	1	1
1	0	1	0	1	0	0	0	1	1	0	1
1	0	1	1	1	0	1	0	1	0	0	1
1	1	0	0	1	1	0	0	0	0	1	1
1	1	0	1	1	1	0	0	1	1	1	1
1	1	1	0	1	1	1	0	0	1	1	1
1	1	1	1	1	1	1	1	0	1	0	1

Figure 5. Simplified Register with Table of Switching Functions

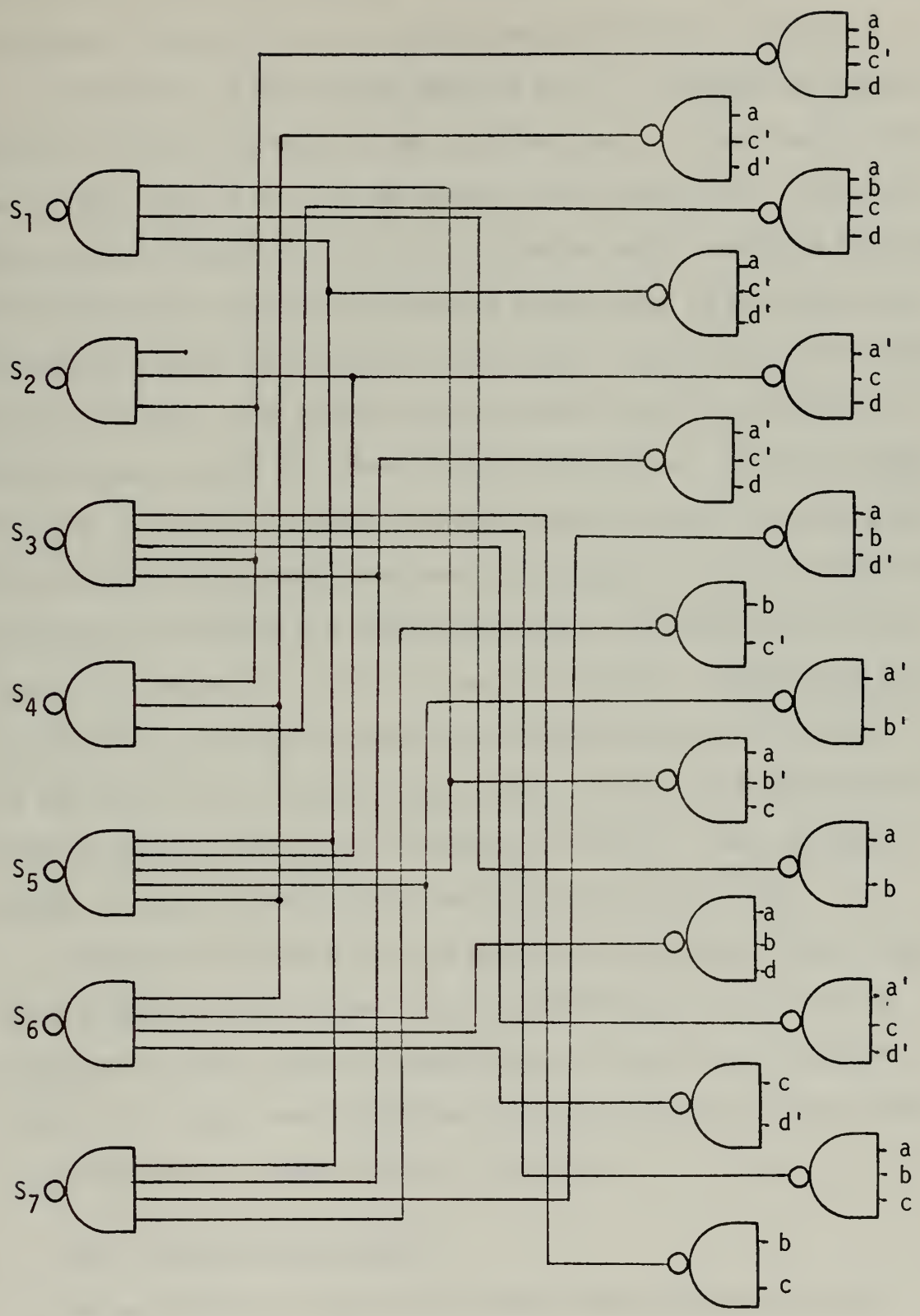


Figure 6. NAND Switch Setting Logic

code pulses have been received. This output can also be used to prevent extraneous code cycling as the pulses are read into the register.

This portion of the unit is shown in Fig. 7. Actuation of the manual switch furnishes one input to the clock AND gate. At the time of turn on a reset pulse is sent to the counter and to the buffer. This sets the switch configuration to Code 0. Assuming normal operation the action is to shift from some Code χ to Code 0 before going to the next code. Therefore if there is a failure in the input circuitry the Code 0 configuration is held. This permits this particular code to be used as a failure back up with the others as operational codes. With no circuit failures the buffer is ready to accept inputs provided one other condition is met. The disable timer must have stepped off its reset (or zero) position and advanced to a prescribed point. The explanation of this feature is presented in detail in the next section. Assuming the timer reaches this point the new input can be transferred into the buffer and at the preset pulse count the input passes through the logic network to furnish setting inputs S_i to transmission gate TG_i. When the manual switch is turned off the static register holds the set code.

In this part of the device the only logical race would occur when the propagation delay between the input (Point A on Fig. 7) and the output of the pulse counter inverter (Point B) was greater than the clock rate. Under these conditions a spurious clock pulse could shift the buffer before a cutoff signal is fed back.

C, TIMER ENABLE/DISABLE CIRCUIT

The selection of a circuit that would furnish the desired time gating is complicated by the large number of choices available. Figure 8 represents one that could be chosen. It is selected because it demonstrates the features such a circuit must incorporate.

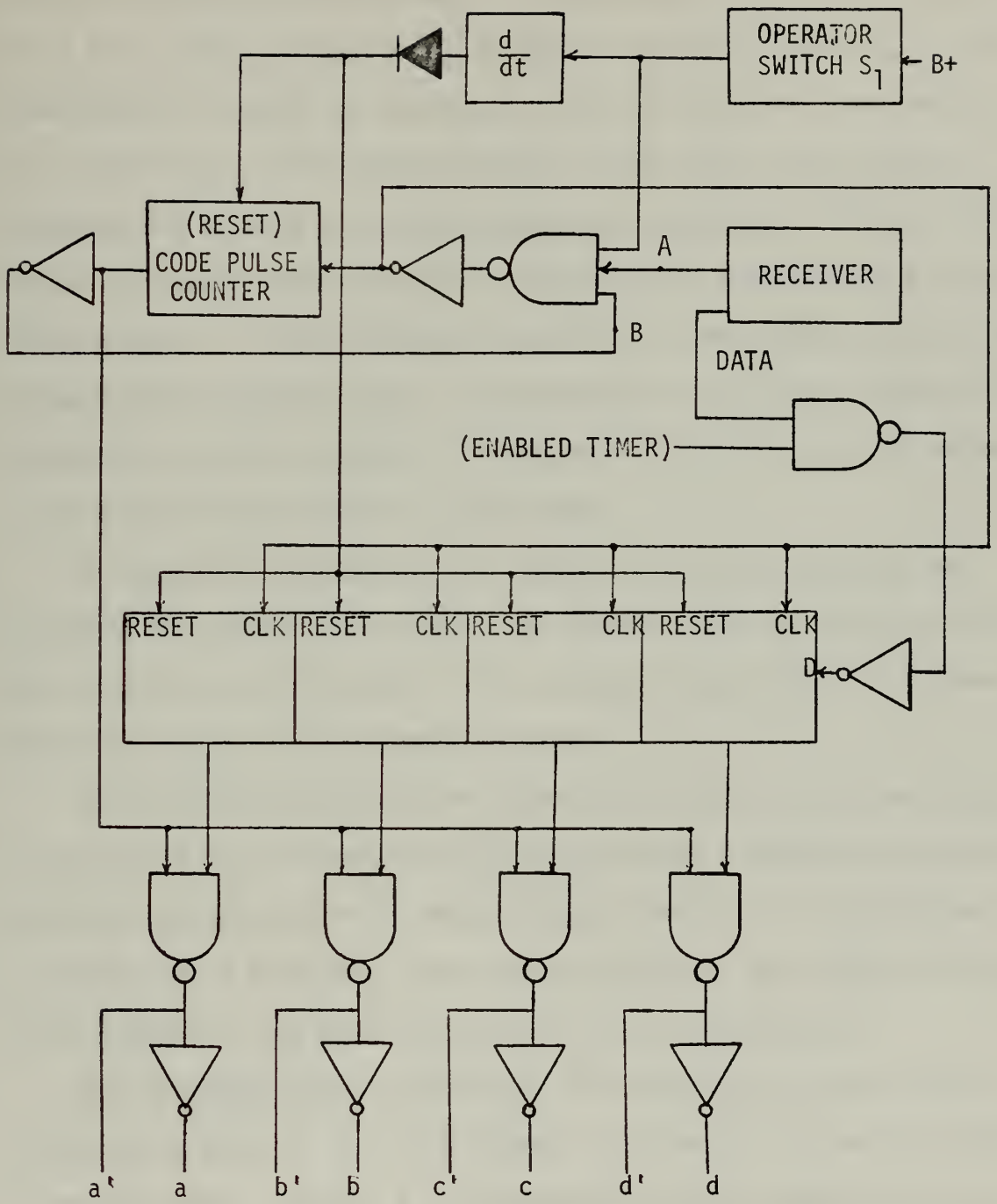


Figure 7. Input Gating and Storage

Its operation is initiated by the same manual code receive switch that is on the buffer clock gate. Closing this switch connects a driver to a free running multivibrator through an opposing diode tee. At the same time the counter is directed to count up from some reset position at a rate f/N_1. If the switch remains on too long a preset count is detected and a pulse is sent to disable the generator. In Fig. 7 this pulse is shown coupled through a set-reset (S-R) flip-flop to a transmission gate. If this electronic switch is in the feedback path of the pseudo-random generator (TG_8), the generator is no longer capable of generating a maximal sequence. Since the S-R flip flop cannot receive a set pulse the gate remains locked open.

The proposed advantage of this method is that the generator may continue to generate some unknown and shorter sequence that will mask the fact that it is disabled. If an alternate description is desired then the output can be directed elsewhere.

If prior to detection of the disable count the code receive switch is placed in the off position the driver remains connected to the multivibrator and the counter is instructed to count down. It continues to count down at a rate f/N_2 until reset is reached. When reset is reached an indication is fed back that turns off the multivibrator.

The reasoning behind selection of this count down feature can be explained by Fig. 9. In (a) the timer is turned on outside the acquisition time range. In Fig. 9, T_c represents the code timespan and N is the disable count. When the timer is left on it reaches generator disable before the code pulses arrive. If the counter resets immediately when turned off the gate may be walked into acquisition as shown in (b). Under these conditions a little a priori knowledge may be used

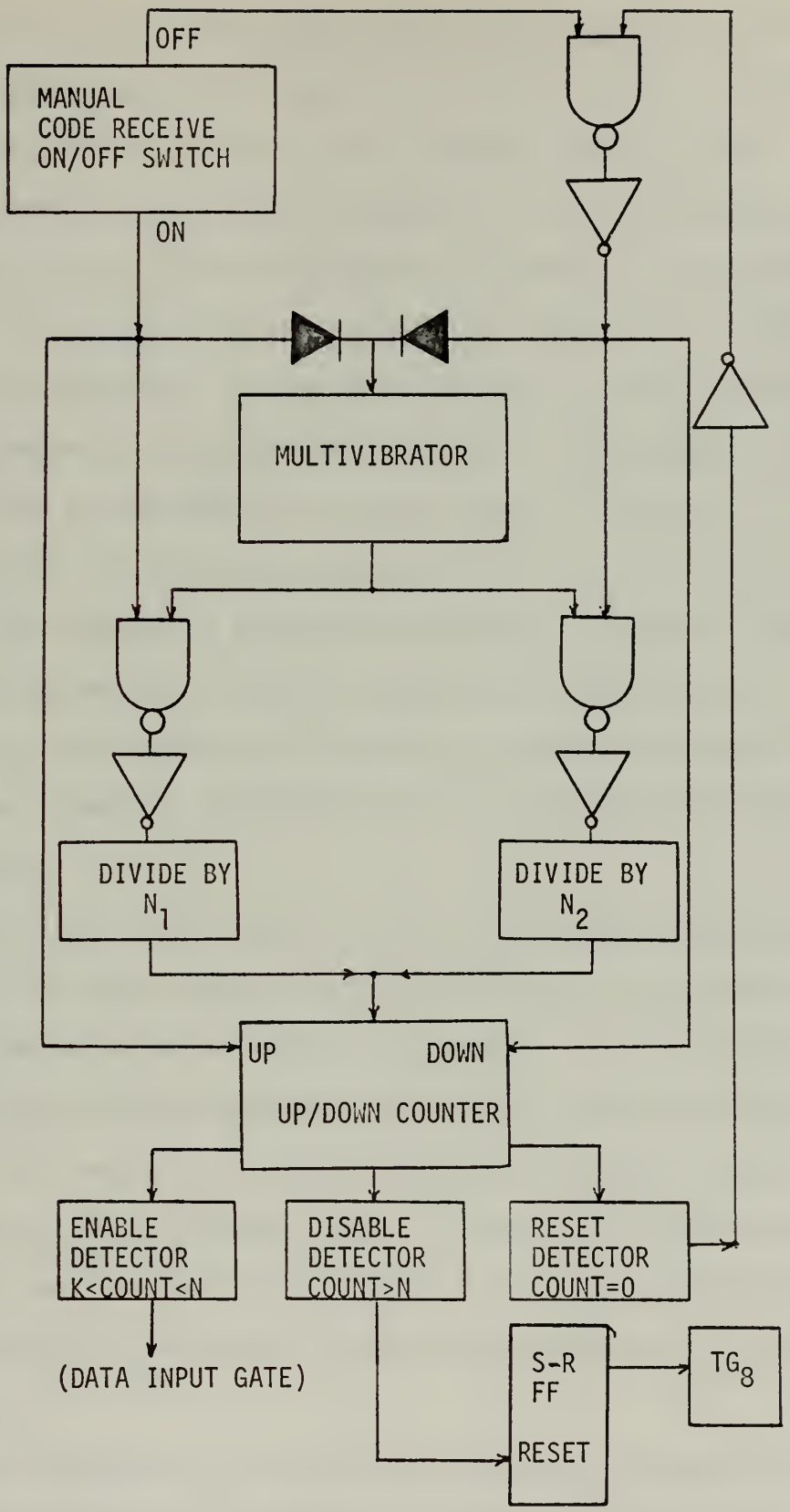


Figure 8. Timer Enable/Disable

to bypass the gate. Note however that in (b) the switch on-off procedure would have to be stopped once acquisition has occurred or the next transition to ON will place the unit in Code 0 mode.

This procedure introduces the possibility that the unauthorized user may be able to detect the success or failure of a code intercept attempt. The countdown feature reduces the search time available when a failure is detected. The countdown results in a count output as shown in Fig. 10 where N_1 and N_2 are assumed equal. If the switch turn off period is for an extended time the count takes the form in (a). Attempts to reduce this off time give an output similar to (b). With $N_2 >> N_1$ the effect is to introduce a dead period following a switch off transition.

Before proceeding it should be pointed out that there is a high probability that tampering will result in a Code 0 transition if the unit is not disabled. Therefore the use of this code should take this into account.

To counteract those situations where simultaneous detection of the presence of an input coding signal and actuation of the switch is possible a third count detector is added to the counter. It is this detector that supplies the previously mentioned input to the buffer receive gate (Fig. 7). Its output is a logical one when the counter steps off its reset position an incremental amount. Therefore the timer not only must be on (i.e. not disabled) it must be on for a certain period of time before the code signal arrives. This is represented by T_b (time blanking) in Fig. 10.

Proper adjustment of the count down and pre-reception count will essentially reduce the probability of an interception to the probability

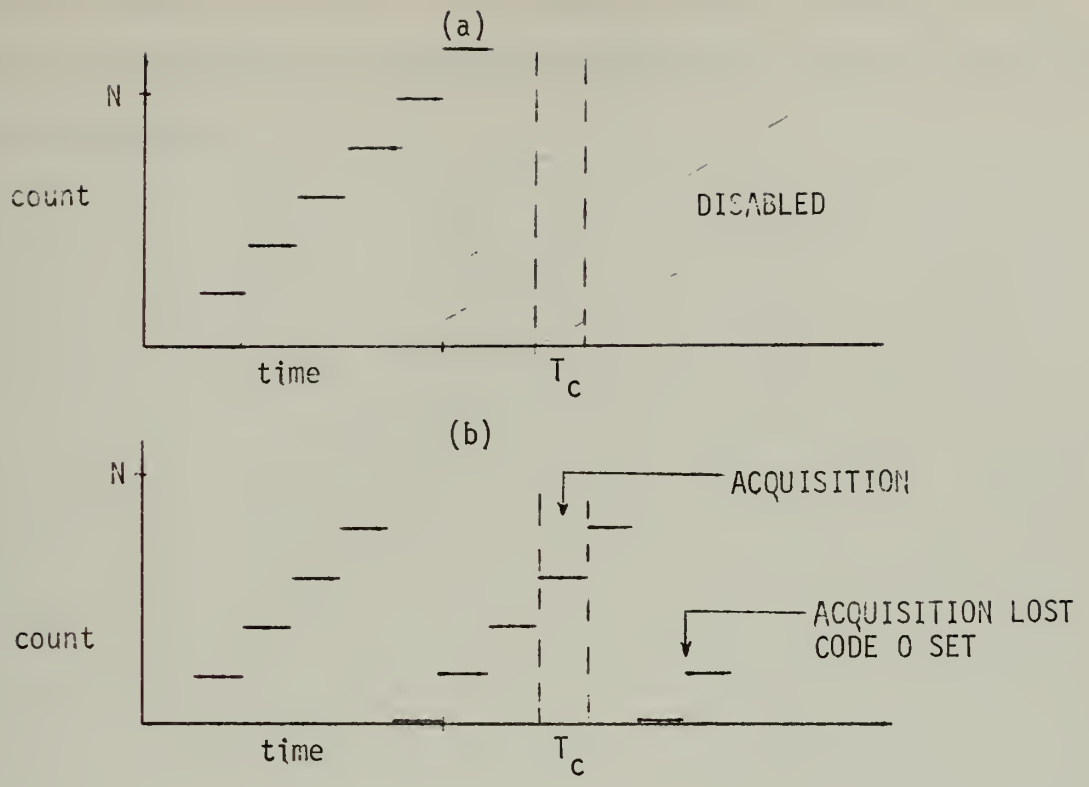


Figure 9. Disable and Walk On Acquisition

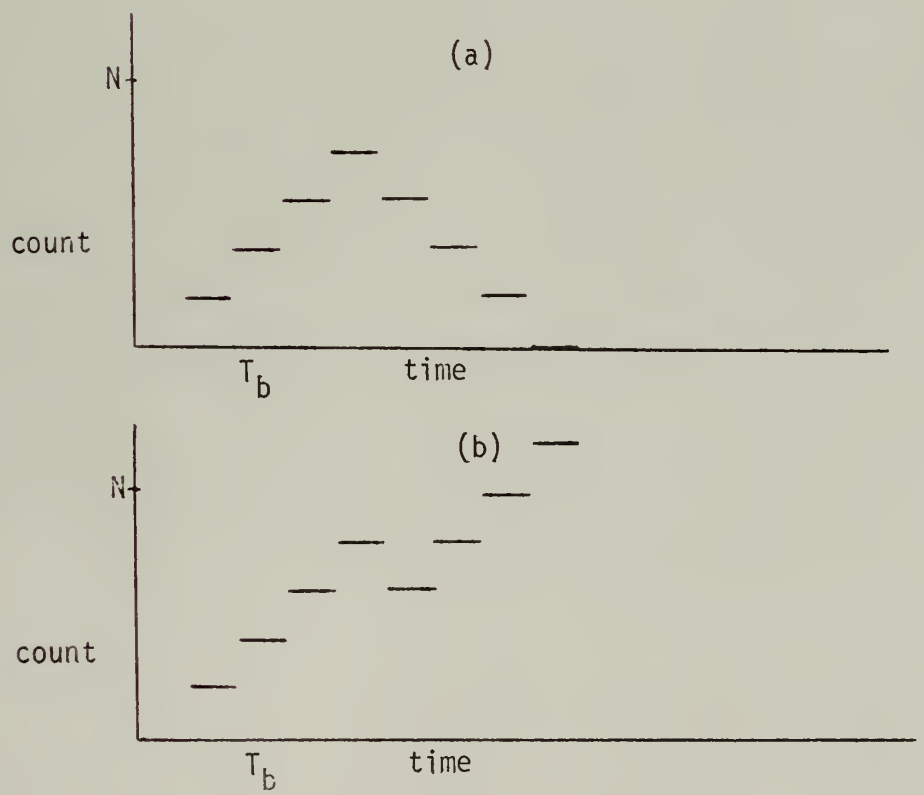


Figure 10. Count Down Feature with Initial Time Blanking

of the success of one trial. This forms the upper probability bound since the probability is reduced when knowledge of the time gate width is not available.

IV. IMPLEMENTATION

The main purpose of this study is to introduce the intended concept and test its logical feasibility rather than to develop a particular technological solution. However there are characteristics of the proposed device that level themselves to general recommendations.

For example, it is apparent that aside from the actual shift register operation the circuitry remains in a static condition for a disproportionate length of time. Therefore a fabrication with a low D.C. power drain is more than normally advantageous. This is particularly true if the device is to be added to an existing piece of battery-powered equipment. For these reasons the new COSMOS IC's with micro-watt power drain are worth considering. In fact except for the RC elements necessary for the disable timer the entire unit could be built with existing IC's described in Ref. 12.

On the other hand for use in a privacy system as much of the unit as possible should be incorporated into a single IC chip or wafer. Again the RC's of the timer present a problem but not an unsolvable one. If this timer cannot be formed as part of the LSIC it can at least be manufactured as a single IC using other than COSMOS techniques. Reference 11 mentions successful fabrication of a low-frequency oscillator using tantalum thin films to form the RC elements.

V. CONCLUSIONS

The conditions imposed are satisfied by this proposal. As a solution of the defined problem it seems realizable. No apparent insurmountable problems were observed that would prevent successful construction.

While the insertion of a gating requirement has implied use in a hostile environment as a privacy-generating device it need not be limited to such use. With suitable modifications the principle could be applied to a discrete address system.

Where a requirement to exclude an unauthorized holder of the device from its use exists there seems to be a high enough degree of assurance that it will be achieved. It should be pointed out however that, unless specially constructed, the device will not give any assurance that a technically intelligent person could not bypass the receive time block. From that viewpoint the device may be classified as a low-level security device. It does give a time frame in which operations may continue with assurance of privacy. What the length of the time frame will be is determined by the ability of the unauthorized user.

From the overall point of view it seems that the major limitation on the unit is the allowable complexity of the switching logic network. Certainly for longer shift registers it does not seem reasonable to expect that all of the possible configurations can be available as in the example. However as many configurations as necessary can be chosen from a large array to establish an operational time span.

This approach has concentrated on the adjustment of the feedback network. The concept could be extended to include setting initial

conditions or even to setting a particular clock rate. With all possibilities included on one coding signal, a multi-dimensional coding choice is available.

LIST OF REFERENCES

1. Golomb, S. W., Shift Register Sequences, Holden-Day, 1967.

2. Martin, R. L., Studies in Feedback-Shift-Register Synthesis of Sequential Machines, MIT Press, 1969.

3. Kautz, W. H., and others, Linear Sequential Switching Circuits Selected Technical Papers, Holden-Day, 1965.

4. Pratt, A. R., "Fast Pseudo-Random Number Generators for Computers," Radio and Electronic Engineer, v. 40, p. 83-88, 2 August 1970.

5. Sergo, J. R. Jr., and Hayes, J. F., "Analysis and Simulation of a PN Synchronization System," IEEE Transactions on Communications Technology, v. COM-18 No. 5, p. 676-679, October 1970.

6. Fracassi, R. D., and Froehlich, F. E., "A Wideband Data Station," IEEE Transactions on Communications Technology, v. COM-14, p. 648-654, October 1966.

7. Huang, T. S., and Tretiak, O. J., "A Pseudorandom Multiplex System for Facsimile Transmission," IEEE Transactions on Communications Technology, v. COM-16, No. 3, p. 436-438, June 1968.

8. Zegers, L. E., "Common Bandwidth Transmissions of Information Signals and Pseudonoise Synchronization Waveforms," IEEE Transactions on Communications Technology, v. COM-16, No. 6, p. 796-807, August 1968.

9. Berlekamp, E. R., Algebraic Coding Theory, McGraw-Hill, 1968.

10. McCluskey, E. J., Introduction to the Theory of Switching Circuits, McGraw-Hill, 1965.

11. Orr, W. H., "An Integrated RC Oscillator for TOUCH-TONE Dialing," IEEE Transactions on Communications Technology, v. COM-16, No. 4, p. 624-628, August 1968.

12. COS/MOS Integrated Circuits Manual, RCA Technical Series CMS-270, 1971.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Documentation Center Cameron Station Alexandria, Virginia 22314	2
2.	Library, Code 0212 Naval Postgraduate School Monterey, California 93940	2
3.	Assoc. Professor G. A. Myers, Code 52 Department of Electrical Engineering Naval Postgraduate School Monterey, California 93940	1
4.	LT Gordon Franklin Gilbert, USN USS Monticello (LSD-35) FPO, San Francisco 96601	1

Security Classification

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1 ORIGINATING ACTIVITY (Corporate author)	2a. REPORT SECURITY CLASSIFICATION
Naval Postgraduate School Monterey, California 93940	Unclassified
	2b. GROUP

3 REPORT TITLE

Design of a Remotely Controlled Pseudo-Random Generator With Local Time Gating

4 DESCRIPTIVE NOTES (Type of report and inclusive dates)

Master's Thesis; December 1971

5 AUTHOR(S) (First name, middle initial, last name)

Gordon Franklin Gilbert, Jr.

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
December 1971	31	12

8a. CONTRACT OR GRANT NO.	9a. ORIGINATOR'S REPORT NUMBER(S)
b. PROJECT NO.	
c.	9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)
d.	

10. DISTRIBUTION STATEMENT

Approved for public release, distribution unlimited.

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY
	Naval Postgraduate School Monterey, California 93940

13. ABSTRACT

This study considers the design of a remote-controlled feedback shift register (pseudo-random sequence generator). A coded sequential input is used to modify existing feedback switch connections. The free running shift register then generates a different maximal length pseudo-random sequence. To prevent control or use of the device by unauthorized persons, a time gate is included in the operation. Recommendations for implementation are presented.

DD FORM 1 NOV 65 1473 (PAGE 1)

S/N 0101-807-6811

Security Classification

A-31408

KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Pseudo-Random Generator						
Local Time Gating						
Remote Controlled Shift Register						
Communications Privacy						
Low-Level Communications Security						

Thesis
G423
c.1
133893
Gilbert
Design of a remotely controlled pseudo-random generator with local time gating.